

J.W. Price 949/261.8433

Yuichi Futa

S.N. 09/603 636



本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

NAK1-BLS3

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1999年 7月16日

出 願 番 号

Application Number:

平成11年特許願第203055号

出 願 人

Applicant(s):

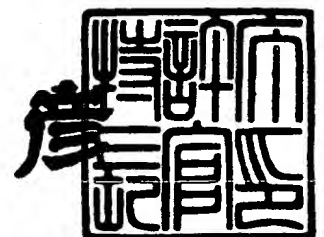
松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 6月29日

特許庁長官
Commissioner,
Patent Office

近 藤 隆 彦



【書類名】 特許願

【整理番号】 2022510334

【提出日】 平成11年 7月16日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 5/00

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 布田 裕一

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【ブルーフの要否】 不要

【書類名】 明細書

【発明の名称】 有限体上の演算装置、逆元演算装置および暗号システム

【特許請求の範囲】

【請求項 1】 予め与えられた有限体 $GF(p)$ (p : 素数) において、正の整数 n と、 $GF(p)$ 上の n 元連立一次方程式のパラメータ $a \downarrow (ij)$ ($1 \leq i, j \leq n$)、 $b \downarrow k$ ($1 \leq k \leq n$) を入力とし、前記方程式の解を出力する有限体上の演算装置であって、

前記連立方程式を行列と第 1 のベクトルで表現し、前記行列と前記第 1 のベクトルを出力する第 1 方程式変換部と、

前記第 1 方程式変換部から出力される前記行列を三角化変換するために、前記行列と前記第 1 のベクトルを変換し、変換された三角行列と第 2 のベクトルを出力する第 2 方程式変換部と、

前記第 2 方程式変換部から出力される前記三角行列の対角成分の $GF(p)$ 上の逆元を出力する逆元演算部と、

前記第 2 方程式変換部から出力される三角行列と前記第 2 のベクトルと、前記逆元演算部から出力される逆元を用いて前記 n 元連立一次方程式の解を求める方程式求解部とを備え、

前記第 2 方程式変換部では、前記有限体の逆元演算を行わないことを特徴とする有限体上の演算装置。

【請求項 2】 前記逆元演算部は、前記第 2 方程式変換部から出力される三角行列の対角成分を $m \downarrow 1$ 、 $m \downarrow 2$ 、...、 $m \downarrow n$ とし、出力する $GF(p)$ 上の逆元を $l \downarrow 1$ 、...、 $l \downarrow n$ とするとき、

$$t \downarrow i = \prod \downarrow (k \neq i) m \downarrow k \bmod p \quad (i=1, 2, \dots, n)$$

と

$$t = \prod \downarrow k m \downarrow k \bmod p$$

を計算する乗算手段と、

$$u = 1/t \bmod p$$

を計算する第 1 逆元演算手段と、

$$l \downarrow i = u \times t \downarrow i \bmod p \quad (i=1, 2, \dots, n)$$

を計算する第 2 逆元演算手段からなることを特徴とする請求項 1 記載の有限体上

の演算装置(ただし、 $x \downarrow 1$ は x の下付き添字が1であることを示す)。

【請求項3】 前記乗算手段は、前記 $t \downarrow i$ ($i=1, 2, \dots, n$)を

$$s \downarrow 1 = m \downarrow 1 \times m \downarrow 2 \bmod p$$

$$s \downarrow 2 = s \downarrow 1 \times m \downarrow 3 \bmod p$$

...

$$s \downarrow (n-3) = s \downarrow (n-4) \times m \downarrow (n-2) \bmod p$$

$$t \downarrow n = s \downarrow (n-3) \times m \downarrow (n-1) \bmod p$$

$$t \downarrow (n-1) = s \downarrow (n-3) \times m \downarrow n \bmod p$$

$$s \downarrow n = m \downarrow (n-1) \times m \downarrow n \bmod p$$

$$t \downarrow (n-2) = s \downarrow (n-4) \times s \downarrow n \bmod p$$

$$s \downarrow (n-1) = m \downarrow (n-2) \times s \downarrow n \bmod p$$

$$t \downarrow (n-3) = s \downarrow (n-5) \times s \downarrow (n-1) \bmod p$$

$$s \downarrow (n-2) = m \downarrow (n-3) \times s \downarrow (n-1) \bmod p$$

$$t \downarrow (n-4) = s \downarrow (n-6) \times s \downarrow (n-2) \bmod p$$

...

$$s \downarrow 5 = m \downarrow 4 \times s \downarrow 6 \bmod p$$

$$t \downarrow 3 = s \downarrow 1 \times s \downarrow 5 \bmod p$$

$$s \downarrow 4 = m \downarrow 3 \times s \downarrow 5 \bmod p$$

$$t \downarrow 2 = m \downarrow 1 \times s \downarrow 4 \bmod p$$

$$t \downarrow 1 = m \downarrow 2 \times s \downarrow 4 \bmod p$$

により計算し、 t を予め与えられた k を用いて、

$$t = t \downarrow k \times m \downarrow k$$

により計算することを特徴とする請求項2記載の有限体上の演算装置。

【請求項4】 予め与えられた有限体 $GF(p)$ の拡大体 $GF(q)$ ($q=p \uparrow n$)において、 $GF(q)$ の元 x を入力とし、 x の $GF(q)$ 上の逆元を出力する逆元演算装置であって、

前記元 x を入力とし、前記元 x の逆元を求めるための連立方程式を生成する方程式生成部と、

前記方程式生成部から出力される連立方程式の解を求める方程式計算部と、

前記方程式計算部の解を x の逆元に変換する逆元変換部とを備え、

前記方程式計算部は請求項 1 記載の有限体上の演算装置であることを特徴とする逆元演算装置(ただし、 $p \uparrow n$ は p の n 乗を示す)。

【請求項 5】 予め与えられた有限体 $GF(p)$ の拡大体 $GF(q)$ ($q=p \uparrow n$)において、 $GF(q)$ の元 x を入力とし、 x の $GF(q)$ 上の逆元を出力する逆元演算装置であって、
前記元 x を入力とし、前記元 x の逆元を求めるための連立方程式を生成する方程式生成部と、
前記方程式生成部から出力される連立方程式の解を求める方程式計算部と、
前記方程式計算部の解を x の逆元に変換する逆元変換部を備え、
前記方程式計算部は請求項 2 記載の有限体上の演算装置であることを特徴とする逆元演算装置。

【請求項 6】 予め与えられた有限体 $GF(p)$ の拡大体 $GF(q)$ ($q=p \uparrow n$)において、 $GF(q)$ の元 x を入力とし、 x の $GF(q)$ 上の逆元を出力する逆元演算装置であって、
前記元 x を入力とし、前記元 x の逆元を求めるための連立方程式を生成する方程式生成部と、
前記方程式生成部から出力される連立方程式の解を求める方程式計算部と、
前記方程式計算部の解を x の逆元に変換する逆元変換部とを備え、
前記方程式計算部は請求項 3 記載の有限体上の演算装置であることを特徴とする逆元演算装置。

【請求項 7】 予め与えられた有限体 $GF(p)$ を利用する有限体利用暗号システムであって、
有限体上の暗号装置と、
正の整数 n と $GF(p)$ 上の n 元連立一次方程式のパラメータ $a \downarrow (ij)$ ($1 \leq i, j \leq n$)、
 $b \downarrow k$ ($1 \leq k \leq n$)を入力とし、前記方程式の解を出力する連立方程式求解装置とを備え、

前記連立方程式求解装置は請求項 1 記載の有限体上の演算装置であることを特徴とする有限体利用暗号システム。

【請求項 8】 予め与えられた有限体 $GF(p)$ を利用する有限体利用暗号システムであって、
有限体を上の暗号装置と、

正の整数 n と $GF(p)$ 上の n 元連立一次方程式のパラメータ $a \downarrow (ij) (1 \leq i, j \leq n)$ 、 $b \downarrow k (1 \leq k \leq n)$ を入力とし、前記方程式の解を出力する連立方程式求解装置とを備え、

前記連立方程式求解装置は請求項 2 記載の有限体上の演算装置であることを特徴とする有限体利用暗号システム。

【請求項 9】 予め与えられた有限体 $GF(p)$ を利用する有限体利用暗号システムであって、

有限体上の暗号装置と、

正の整数 n と $GF(p)$ 上の n 元連立一次方程式のパラメータ $a \downarrow (ij) (1 \leq i, j \leq n)$ 、 $b \downarrow k (1 \leq k \leq n)$ を入力とし、前記方程式の解を出力する連立方程式求解装置とを備え、

前記連立方程式求解装置は請求項 3 記載の有限体上の演算装置であることを特徴とする有限体利用暗号システム。

【請求項 10】 予め与えられた有限体 $GF(p)$ の拡大体 $GF(q) (q=p \uparrow n)$ を利用する拡大体利用暗号システムであって、

拡大体上の暗号装置と、

$GF(q)$ の元 x を入力とし、 x の $GF(q)$ 上の逆元を出力する逆元演算装置とを備え、

前記逆元演算装置は請求項 4 記載の逆元演算装置であることを特徴とする拡大体利用暗号システム。

【請求項 11】 予め与えられた有限体 $GF(p)$ の拡大体 $GF(q) (q=p \uparrow n)$ を利用する拡大体利用暗号システムであって、

拡大体上の暗号装置と、

$GF(q)$ の元 x を入力とし、 x の $GF(q)$ 上の逆元を出力する逆元演算装置とを備え、

前記逆元演算装置は請求項 5 記載の逆元演算装置であることを特徴とする拡大体利用暗号システム。

【請求項 12】 予め与えられた有限体 $GF(p)$ の拡大体 $GF(q) (q=p \uparrow n)$ を利用する拡大体利用暗号システムであって、

拡大体上の暗号装置と、

$GF(q)$ の元 x を入力とし、 x の $GF(q)$ 上の逆元を出力する逆元演算装置とを備え、

前記逆元演算装置は請求項6記載の逆元演算装置であることを特徴とする拡大体利用暗号システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は情報セキュリティ技術としての暗号技術及び、誤り訂正技術に関するものであり、特に、拡大体および連立方程式を用いて実現する暗号及びデジタル署名技術、誤り訂正技術に関するものである。

【0002】

【従来の技術】

秘密通信方式とは、特定の通信相手以外に通信内容を漏らすことなく通信を行なう方式である。またデジタル署名方式とは、通信相手に通信内容の正当性を示したり、本人であることを証明する通信方式である。この署名方式には公開鍵暗号とよばれる暗号方式を用いる。公開鍵暗号は通信相手が多数の時、通信相手ごとに異なる暗号鍵を容易に管理するための方式であり、多数の通信相手と通信を行なうのに不可欠な基盤技術である。簡単に説明すると、これは暗号化鍵と復号化鍵が異なり、復号化鍵は秘密にするが、暗号化鍵を公開する方式である。この公開鍵暗号の安全性の根拠に用いられるものに離散対数問題がある。離散対数問題には代表的に、有限体上定義されるもの及び楕円曲線上定義されるものがある。これはNeal Koblitz, "A Course in Number theory and Cryptography", Springer-Verlag, 1987に詳しく述べられている。楕円曲線上の離散対数問題を以下に述べる。

【0003】

楕円曲線上の離散対数問題とは、

E を有限体 $GF(q)$ ($q=p \uparrow n$, p :素数)上定義された楕円曲線とし、 E の位数が大きな素数で割れる元 G をベースポイントとする($p \uparrow n$ は p の n 乗を示す)。このとき、 E の与えられた元 Y に対して、

$$Y=x * G$$

となる整数 x が存在するならば x を求めよ、という問題である(ここで、 $x * G$ は G を

x 回楕円曲線の加算を行うことを意味する)。ここで、 $GF(q)$ は $GF(p)$ の拡大体である。拡大体については、岡本龍明、山本博資、“現代暗号”、シリーズ／情報科学の数学、産業図書、1997、26～28ページに詳しく述べられている。

【0004】

(従来例1)

以下に上記楕円曲線上の離散対数問題を応用したエルガマル署名について、図6を用いて説明する。

【0005】

この図は、上記エルガマル署名によるデジタル署名方式の手順を示すシーケンス図である。

【0006】

ユーザA310、管理センタ320及びユーザB330は、ネットワークで接続されている。

【0007】

p を素数、 $q=p \uparrow n$ 、有限体 $GF(q)$ 上の楕円曲線を E とする。 E のベースポイントを G とし、 G の位数を r とする。すなわち、 r は、

$$r * G = 0$$

を満たす最小の正整数である。ただし、 0 は楕円曲線の群の加算における零元である。

【0008】

(1)管理センタ320による公開鍵の生成

管理センタ320は、予め通知されているユーザA310の秘密鍵 $x \downarrow A$ を用いて、次の式より、ユーザA310の公開鍵を作成する(ステップS1～S2)。

【0009】

$$Y \downarrow A = x \downarrow A * G$$

その後、管理センタ320は、有限体 $GF(q)$ 、楕円曲線 E 及びベースポイント G をシステムパラメータとして公開し、他のユーザB330にユーザA310の公開鍵 $Y \downarrow A$ を公開する(ステップS3～S4)。

【0010】

(2) ユーザA310による署名生成

ユーザA310は、乱数 k を生成する(ステップS5)。

【0011】

次に、ユーザA310は、

$$R \downarrow 1 = (r \downarrow x, r \downarrow y) = k * G$$

を計算し(ステップS6)、

$$s \times k = m + r \downarrow x \times x \downarrow A \pmod r$$

から、 s を計算する(ステップS7)。ここで、 m は、ユーザA310がユーザB330へ送信するメッセージである。

【0012】

さらに、ユーザA310は、得られた $(R \downarrow 1, s)$ を署名としてメッセージ m とともに、ユーザB330へ送信する(ステップS8)。

【0013】

(3) ユーザB330による署名検証

ユーザB330は、

$$s * R \downarrow 1 = m * G + r \downarrow x * Y \downarrow A$$

が成立するかどうか判定することにより、送信者であるユーザA310の身元を確認する(ステップS9)。これは、

$$s * R \downarrow 1 = [(m + r \downarrow x \times x \downarrow A) / k] \times k * G$$

$$= (m + r \downarrow x \times x \downarrow A) * G$$

$$= m * G + (r \downarrow x \times x \downarrow A) * G$$

$$= m * G + r \downarrow x * Y \downarrow A$$

となることから明らかである。

【0014】

上記に示した楕円曲線上の離散対数問題を応用したエルガマル署名によるデジタル署名方式における公開鍵の生成、署名生成、署名検証のそれぞれにおいて、楕円曲線上の点の冪倍の演算が行われる。

【0015】

楕円曲線の演算公式については、

Miyaji, Ono, and Cohen,

"Efficient elliptic curve exponentiation",

Advances in cryptology-proceedings of ICICS' 97,

Lecture notes in computer science, 1997, Springer-verlag, 282-290.

に詳しく説明されている。

【0016】

楕円曲線の方程式を

$$y^2 = x^3 + ax + b$$

とする。任意の楕円曲線上の点Pの座標を $(x \downarrow 1, y \downarrow 1)$ とする。この座標はアフィン座標と呼ばれ、楕円曲線の加算に有限体 $GF(q)$ の逆元演算の処理を含むことが知られている。上記の論文では、射影座標と呼ばれる座標に触れているが、これは、

$$(x \downarrow 1, y \downarrow 1) \rightarrow (x \downarrow 1, y \downarrow 1, 1)$$

と2項組座標を3項組座標に対応づけるものである。逆に、

$$(X, Y, Z) \rightarrow (X/Z, Y/Z)$$

と対応する。3項組座標の場合、楕円曲線の加算に有限体 $GF(q)$ の逆元演算の処理を含まない。一般に有限体の逆元演算は、計算時間が大きいので、3項組座標をよく用いられる。

【0017】

しかし、この座標もエルガマル署名に使用する場合は、ステップS6のようにアフィン座標に変換する必要がある。したがって、この場合も逆元演算が必要になる。

【0018】

このため、逆元演算の処理時間を削減することは、楕円曲線暗号の高速化につながる。しかし、従来の逆元演算法は処理時間が長いという問題がある。

【0019】

(従来例2)

以下で、従来の拡大体 $GF(q)$ ($q = p^n$, p :素数)の逆元演算について図7を用いて説明する。ここで、簡単のため拡大体 $GF(q)$ の生成多項式を $f(g) = g^n - \beta$ とし

、生成多項式の根を α とする。入力となる $GF(q)$ の元を $x = x \downarrow 0 + x \downarrow 1 \times \alpha + \dots + x \downarrow (n-1) \times \alpha \uparrow (n-1)$ とする。

【0020】

step1: 方程式生成部401

x から以下の $y \downarrow i (0 \leq i \leq n-1)$ に関する連立方程式を生成する。

【0021】

$x \downarrow 0 \times y \downarrow 0 + \beta \times x \downarrow (n-1) \times y \downarrow 1 + \beta \times x \downarrow (n-2) \times y \downarrow 2 + \dots + \beta \times x \downarrow 1 \times y \downarrow (n-1) = 1$

$x \downarrow 1 \times y \downarrow 0 + x \downarrow 0 \times y \downarrow 1 + \beta \times x \downarrow (n-1) \times y \downarrow 2 + \dots + \beta \times x \downarrow 2 \times y \downarrow (n-1) = 0$

$x \downarrow 2 \times y \downarrow 0 + x \downarrow 1 \times y \downarrow 1 + x \downarrow 0 \times y \downarrow 2 + \dots + \beta \times x \downarrow 3 \times y \downarrow (n-1) = 0$

...

$x \downarrow (n-1) \times y \downarrow 0 + x \downarrow (n-2) \times y \downarrow 1 + x \downarrow (n-3) \times y \downarrow 2 + \dots + x \downarrow 0 \times y \downarrow (n-1) = 0$

step2: 方程式計算部402

方程式生成部401で生成した方程式の解 $y \downarrow k (0 \leq k \leq n-1)$ を求める。

【0022】

step3: 逆元変換部403

方程式計算部402で求めた解 $y \downarrow k (0 \leq k \leq n-1)$ を逆元 $I = y \downarrow 0 + y \downarrow 1 \times \alpha + \dots + y \downarrow (n-1) \times \alpha \uparrow (n-1)$ に変換する。

【0023】

上記の I と x について、

$x \times I = 1 \pmod{f(g)}$

という関係式であるとき、

$x \times I = x \downarrow 0 \times (y \downarrow 0 + y \downarrow 1 \times \alpha + \dots + y \downarrow (n-1) \times \alpha \uparrow (n-1))$

$+ x \downarrow 1 \times \alpha \times (y \downarrow 0 + y \downarrow 1 \times \alpha + \dots + y \downarrow (n-1) \times \alpha \uparrow (n-1))$

$+ x \downarrow 2 \times \alpha \uparrow 2 \times (y \downarrow 0 + y \downarrow 1 \times \alpha + \dots + y \downarrow (n-1) \times \alpha \uparrow (n-1))$

...

$+ x \downarrow (n-1) \times \alpha \uparrow (n-1) \times (y \downarrow 0 + y \downarrow 1 \times \alpha + \dots + y \downarrow (n-1) \times \alpha \uparrow (n-1))$

であり、

$\alpha \uparrow n = \beta \pmod{f(g)}$

であるので、

$$\begin{aligned} x \times I &= x \downarrow 0 \times (y \downarrow 0 + y \downarrow 1 \times \alpha + \dots + y \downarrow (n-1) \times \alpha \uparrow (n-1)) \\ &\quad + x \downarrow 1 \times (y \downarrow 0 \times \alpha + y \downarrow 1 \times \alpha \uparrow 2 + \dots + y \downarrow (n-1) \times \beta) \\ &\quad + x \downarrow 2 \times (y \downarrow 0 \times \alpha \uparrow 2 + y \downarrow 1 \times \alpha \uparrow 3 + \dots + y \downarrow (n-1) \times \alpha \times \beta) \\ &\quad \dots \\ &\quad + x \downarrow (n-1) \times (y \downarrow 0 \times \alpha \uparrow (n-1) + y \downarrow 1 \times \beta + \dots + y \downarrow (n-1) \times \alpha \uparrow (n-2) \beta) \end{aligned}$$

であり、 α の降冪の順に整理すると

$$\begin{aligned} x \times I &= x \downarrow 0 \times y \downarrow 0 + \beta \times x \downarrow (n-1) \times y \downarrow 1 + \dots + \beta \times x \downarrow 1 \times y \downarrow (n-1) \\ &\quad + \alpha \times (x \downarrow 1 \times y \downarrow 0 + x \downarrow 0 \times y \downarrow 1 + \dots + \beta \times x \downarrow 2 \times y \downarrow (n-1)) \\ &\quad + \alpha \uparrow 2 \times (x \downarrow 2 \times y \downarrow 0 + x \downarrow 1 \times y \downarrow 1 + \dots + \beta \times x \downarrow 3 \times y \downarrow (n-1)) \\ &\quad \dots \\ &\quad + \alpha \uparrow (n-1) \times (x \downarrow (n-1) \times y \downarrow 0 + x \downarrow (n-2) \times y \downarrow 1 + \dots + x \downarrow 0 \times y \downarrow (n-1)) \end{aligned}$$

である。これが1に等しいので、上記例の方程式生成部401によって生成された方程式が導くことができる。したがって、拡大体GF(q)の逆元を求めることは、基礎体GF(p)上の連立方程式を解くことと等しい。

【0 0 2 4】

また、上記例では、 $g \uparrow n - \beta$ の形の生成多項式を扱ったが、一般の生成多項式に対しても同様の操作により、方程式を生成できる。

【0 0 2 5】

(従来例 3)

以下で、従来の基礎体GF(p)上の連立方程式の解法について図 8 を用いて説明する。この解法は、ガウスの消去法と呼ばれる。ガウスの消去法については、水上孝一編著、「コンピュータによる数値計算」、プログラミング入門シリーズ、朝倉書店、1985、76～82ページに詳しく述べられている。

【0 0 2 6】

$x \downarrow k (1 \leq k \leq n)$ に対する連立方程式を、

$$a \downarrow (11) \times x \downarrow 1 + a \downarrow (12) \times x \downarrow 2 + \dots + a \downarrow (1n) \times x \downarrow n = b \downarrow 1$$

$$a \downarrow (21) \times x \downarrow 1 + a \downarrow (22) \times x \downarrow 2 + \dots + a \downarrow (2n) \times x \downarrow n = b \downarrow 2$$

...

$$a \downarrow (n1) \times x \downarrow 1 + a \downarrow (n2) \times x \downarrow 2 + \dots + a \downarrow (nn) \times x \downarrow n = b \downarrow n$$

とし、この解を求める。

【 0 0 2 7 】

step1: 第 1 方程式変換部501

行列M、ベクトルz、vを以下のようにおく。

【 0 0 2 8 】

$M = (a \downarrow (ij))$ を第 i 行第 j 列の成分とする行列)

$v = (b \downarrow k)$ を第 k 行の成分とする縦ベクトル)

step2: 第 2 方程式変換部502

行列Mを三角化するように方程式、すなわち、行列M、vを変換する。

【 0 0 2 9 】

step3: 方程式求解部503

第 2 方程式変換部502によって変換された行列M、ベクトルvを用いて、方程式の解を求める。

【 0 0 3 0 】

上記例の第 1 方程式変換部501において、ベクトルXを

$X = (x \downarrow k)$ を第 k 行の成分とする縦ベクトル)

とするとき、

$$M \cdot X = v$$

が成り立つ。ただし、 \cdot は行列とベクトルの乗算である。第 1 方程式変換部501は、このように方程式を上式のような行列で表せる式に変換していることになる。

【 0 0 3 1 】

第 2 方程式変換部502では、方程式の解を変化しない変換により、行列を上三角行列に変換する。このとき、この上三角行列の対角成分は1である。詳しくは上記文献を参照していただきたい。対角成分を1にするため、基礎体の逆元演算がn回と乗算が $1/2 \times n \times (n-1)$ 回必要になる。その他、行列の下三角を0にするために、基礎体の乗算が $1/3 \times n \times (n-1) \times (n+1)$ 回必要になる。基礎体の乗算、逆元演算の計算量をそれぞれ、Mul、Invとすると、第 2 方程式変換部502の計算量

は、

$$1/6 \times n \times (2 \times n \uparrow 2 + 3 \times n - 5) \times \text{Mul} + n \times \text{Inv}$$

である。

【0 0 3 2】

方程式求解部503は、第2方程式変換部502で行列が対角成分1の上三角行列に変換されているため、 $x \downarrow n$ から $x \downarrow 1$ まで順番に簡単な計算で解を求めることができる。この計算量は、 $1/2 \times n \times (n+1) \times \text{Mul}$ である。

【0 0 3 3】

以上より、従来例3の全計算量は、

$$1/3 \times n \times (n \uparrow 2 + 3 \times n - 1) \times \text{Mul} + n \times \text{Inv}$$

である。このように基礎体の逆元演算が多くなる。一般に基礎体の逆元演算は計算量が大きいため、従来例3の全体の計算量が大きくなるという問題がある。

【0 0 3 4】

【発明が解決しようとする課題】

暗号システムにおいて、高速な有限体上の連立方程式の求解及び、拡大体上の逆元演算を実現することは重要である。従来技術である有限体上の連立方程式の求解法においては、基礎体の逆元演算の計算量が大きいうという欠点がある。

【0 0 3 5】

本発明は、以上の従来技術における問題点を鑑みて行われたもので、基礎体の逆元演算の回数を削減することにより、有限体上の連立方程式の求解及び、拡大体上の逆元演算の計算時間を短縮し、これにより高速な暗号方式、署名方式を提供することを目的とする。

【0 0 3 6】

【課題を解決するための手段】

請求項1における発明は、予め与えられた有限体 $GF(p)$ (p :素数)において、正の整数 n と、 $GF(p)$ 上の n 元連立一次方程式のパラメータ $a \downarrow (ij)$ ($1 \leq i, j \leq n$)、 $b \downarrow k$ ($1 \leq k \leq n$)を入力とし、前記方程式の解を出力する有限体上の演算装置であって、前記連立方程式を行列と第1のベクトルで表現し、前記行列と前記第1のベクトルを出力する第1方程式変換部と、前記第1方程式変換部から出力される前

記行列を三角化変換するために、前記行列と前記第1のベクトルを変換し、変換された三角行列と第2のベクトルを出力する第2方程式変換部と、前記第2方程式変換部から出力される前記三角行列の対角成分のGF(p)上の逆元を出力する逆元演算部と、前記第2方程式変換部から出力される三角行列と前記第2のベクトルと、前記逆元演算部から出力される逆元を用いて前記n元連立一次方程式の解を求める方程式求解部を備え、前記第2方程式変換部では、前記有限体の逆元演算を行わないことを特徴とする。

【0037】

請求項2における発明は、請求項1の逆元演算部は、前記第2方程式変換部から出力される三角行列の対角成分を $m \downarrow 1, m \downarrow 2, \dots, m \downarrow n$ とし、出力するGF(p)上の逆元を $l \downarrow 1, \dots, l \downarrow n$ とすると、 $t \downarrow i = \prod_{k \neq i} m \downarrow k \bmod p$ ($i=1, 2, \dots, n$)と $t = \prod_{k=1}^n m \downarrow k \bmod p$ を計算する乗算手段と、 $u = 1/t \bmod p$ を計算する第1逆元演算手段と、 $l \downarrow i = u \times t \downarrow i \bmod p$ ($i=1, 2, \dots, n$)を計算する第2逆元演算手段からなることを特徴とする(ただし、 $x \downarrow 1$ はxの下付き添字が1であることを示す)。

【0038】

請求項3における発明は、請求項2の乗算手段は、前記 $t \downarrow i$ ($i=1, 2, \dots, n$)を $s \downarrow 1 = m \downarrow 1 \times m \downarrow 2 \bmod p, s \downarrow 2 = s \downarrow 1 \times m \downarrow 3 \bmod p, \dots, s \downarrow (n-3) = s \downarrow (n-4) \times m \downarrow (n-2) \bmod p, t \downarrow n = s \downarrow (n-3) \times m \downarrow (n-1) \bmod p, t \downarrow (n-1) = s \downarrow (n-3) \times m \downarrow n \bmod p, s \downarrow n = m \downarrow (n-1) \times m \downarrow n \bmod p, t \downarrow (n-2) = s \downarrow (n-4) \times s \downarrow n \bmod p, s \downarrow (n-1) = m \downarrow (n-2) \times s \downarrow n \bmod p, t \downarrow (n-3) = s \downarrow (n-5) \times s \downarrow (n-1) \bmod p, s \downarrow (n-2) = m \downarrow (n-3) \times s \downarrow (n-1) \bmod p, t \downarrow (n-4) = s \downarrow (n-6) \times s \downarrow (n-2) \bmod p, \dots, s \downarrow 5 = m \downarrow 4 \times s \downarrow 6 \bmod p, t \downarrow 3 = s \downarrow 1 \times s \downarrow 5 \bmod p, s \downarrow 4 = m \downarrow 3 \times s \downarrow 5 \bmod p, t \downarrow 2 = m \downarrow 1 \times s \downarrow 4 \bmod p, t \downarrow 1 = m \downarrow 2 \times s \downarrow 4 \bmod p$ により計算し、tを予め与えられたkを用いて、 $t = t \downarrow k \times m \downarrow k$ により計算することを特徴とする。

【0039】

請求項4における発明は、予め与えられた有限体GF(p)の拡大体GF(q) ($q=p \uparrow n$)において、GF(q)の元xを入力とし、xのGF(q)上の逆元を出力する逆元演算装置であって、前記元xを入力とし、前記元xの逆元を求めるための連立方程式を生成す

る方程式生成部と、前記方程式生成部から出力される連立方程式の解を求める方程式計算部と、前記方程式計算部の解を x の逆元に変換する逆元変換部を備え、前記方程式計算部は請求項 1 記載の有限体上の演算装置であることを特徴とする（ただし、 $p \uparrow n$ は p の n 乗を示す）。

【0040】

請求項 5 における発明は、予め与えられた有限体 $GF(p)$ の拡大体 $GF(q)$ ($q=p \uparrow n$) において、 $GF(q)$ の元 x を入力とし、 x の $GF(q)$ 上の逆元を出力する逆元演算装置であって、前記元 x を入力とし、前記元 x の逆元を求めるための連立方程式を生成する方程式生成部と、前記方程式生成部から出力される連立方程式の解を求める方程式計算部と、前記方程式計算部の解を x の逆元に変換する逆元変換部を備え、前記方程式計算部は請求項 2 記載の有限体上の演算装置であることを特徴とする。

【0041】

請求項 6 における発明は、予め与えられた有限体 $GF(p)$ の拡大体 $GF(q)$ ($q=p \uparrow n$) において、 $GF(q)$ の元 x を入力とし、 x の $GF(q)$ 上の逆元を出力する逆元演算装置であって、前記元 x を入力とし、前記元 x の逆元を求めるための連立方程式を生成する方程式生成部と、前記方程式生成部から出力される連立方程式の解を求める方程式計算部と、前記方程式計算部の解を x の逆元に変換する逆元変換部を備え、前記方程式計算部は請求項 3 記載の有限体上の演算装置であることを特徴とする。

【0042】

請求項 7 における発明は、予め与えられた有限体 $GF(p)$ を利用する有限体利用暗号システムであって、有限体上の暗号装置と、正の整数 n と $GF(p)$ 上の n 元連立一次方程式のパラメータ $a \downarrow (ij)$ ($1 \leq i, j \leq n$)、 $b \downarrow k$ ($1 \leq k \leq n$)を入力とし、前記方程式の解を出力する連立方程式求解装置を備え、前記連立方程式求解装置は請求項 1 記載の有限体上の演算装置であることを特徴とする。

【0043】

請求項 8 における発明は、予め与えられた有限体 $GF(p)$ を利用する有限体利用暗号システムであって、有限体を上の暗号装置と、正の整数 n と $GF(p)$ 上の n 元連

立一次方程式のパラメータ $a \downarrow (ij) (1 \leq i, j \leq n)$ 、 $b \downarrow k (1 \leq k \leq n)$ を入力とし、前記方程式の解を出力する連立方程式求解装置を備え、前記連立方程式求解装置は請求項 2 記載の有限体上の演算装置であることを特徴とする。

【0044】

請求項 9 における発明は、予め与えられた有限体 $GF(p)$ を利用する有限体利用暗号システムであって、有限体上の暗号装置と、正の整数 n と $GF(p)$ 上の n 元連立一次方程式のパラメータ $a \downarrow (ij) (1 \leq i, j \leq n)$ 、 $b \downarrow k (1 \leq k \leq n)$ を入力とし、前記方程式の解を出力する連立方程式求解装置を備え、前記連立方程式求解装置は請求項 3 記載の有限体上の演算装置であることを特徴とする。

【0045】

請求項 10 における発明は、予め与えられた有限体 $GF(p)$ の拡大体 $GF(q) (q=p \uparrow n)$ を利用する拡大体利用暗号システムであって、拡大体上の暗号装置と、 $GF(q)$ の元 x を入力とし、 x の $GF(q)$ 上の逆元を出力する逆元演算装置を備え、前記逆元演算装置は請求項 4 記載の逆元演算装置であることを特徴とする。

【0046】

請求項 11 における発明は、予め与えられた有限体 $GF(p)$ の拡大体 $GF(q) (q=p \uparrow n)$ を利用する拡大体利用暗号システムであって、拡大体上の暗号装置と、 $GF(q)$ の元 x を入力とし、 x の $GF(q)$ 上の逆元を出力する逆元演算装置を備え、前記逆元演算装置は請求項 5 記載の逆元演算装置であることを特徴とする。

【0047】

請求項 12 における発明は、予め与えられた有限体 $GF(p)$ の拡大体 $GF(q) (q=p \uparrow n)$ を利用する拡大体利用暗号システムであって、拡大体上の暗号装置と、 $GF(q)$ の元 x を入力とし、 x の $GF(q)$ 上の逆元を出力する逆元演算装置を備え、前記逆元演算装置は請求項 6 記載の逆元演算装置であることを特徴とする。

【0048】

【発明の実施の形態】

(実施形態 1)

図 1 は、実施形態 1 における有限体上の演算装置の構成を示すブロック図である。

【 0 0 4 9 】

この有限体上の演算装置は、予め与えられた体 $GF(p)$ (p :素数)において、正の整数 n と以下の n 元連立一次方程式のパラメータ $a \downarrow (ij)$ ($1 \leq i, j \leq n$)、 $b \downarrow k$ ($1 \leq k \leq n$)を与えられたとき、前記方程式の $GF(p)$ 上の解を出力するものである。

【 0 0 5 0 】

$$a \downarrow (11) \times x \downarrow 1 + a \downarrow (12) \times x \downarrow 2 + \dots + a \downarrow (1n) \times x \downarrow n = b \downarrow 1$$

$$a \downarrow (21) \times x \downarrow 1 + a \downarrow (22) \times x \downarrow 2 + \dots + a \downarrow (2n) \times x \downarrow n = b \downarrow 2$$

...

$$a \downarrow (n1) \times x \downarrow 1 + a \downarrow (n2) \times x \downarrow 2 + \dots + a \downarrow (nn) \times x \downarrow n = b \downarrow n$$

有限体上の演算装置10は、第1方程式変換部101と、第2方程式変換部102と、逆元演算部103と、方程式求解部104を備える。

【 0 0 5 1 】

第1方程式変換部101は、 n と $a \downarrow (ij)$ ($1 \leq i, j \leq n$)、 $b \downarrow k$ ($1 \leq k \leq n$)を入力とし、それらの方程式のパラメータを以下の行列 $M[1]$ とベクトル $v[1]$ に変換し、出力する。

【 0 0 5 2 】

$M[1] = (a \downarrow (ij))$ を第 i 行第 j 列の成分とする行列)

$v[1] = (b \downarrow k)$ を第 k 行の成分とする縦ベクトル)

第2方程式変換部102は、第1方程式変換部101から出力された行列 $M[1]$ とベクトル $v[1]$ を行列 $M[1]$ が三角化されるように変換し、変換された行列 $M[2]$ とベクトル $v[2]$ を出力する。

【 0 0 5 3 】

逆元演算部103は、第2方程式変換部102から出力された行列 $M[2]$ の対角成分 $m \downarrow k$ ($1 \leq k \leq n$)の $GF(p)$ 上の逆元 $I \downarrow k$ を計算し、出力する。

【 0 0 5 4 】

方程式求解部104は、第2方程式変換部102から出力された行列 $M[2]$ とベクトル $v[2]$ と逆元演算部103から出力された逆元 $I \downarrow k$ ($1 \leq k \leq n$)を用いて、方程式の解を求め出力する。

【 0 0 5 5 】

(第 1 方程式変換部101の検証)

ベクトル $x[1]$ を以下のように定義する。

【0 0 5 6】

$x[1] = (x \downarrow k \text{ を第 } k \text{ 行の成分とする縦ベクトル})$

このとき、

$M[1] \cdot x[1] = v[1]$

が成り立つ。ただし、 \cdot は行列とベクトルの乗算である。第 1 方程式変換部101は、このように方程式を上式のような行列で表せる式に変換していることになる。

【0 0 5 7】

(第 2 方程式変換部102の構成)

図 2 は、第 2 方程式変換部102の構成を示すブロック図である。

【0 0 5 8】

第 2 方程式変換部102は、第 1 方程式変換部101から出力された行列 $M[1]$ とベクトル $v[1]$ を行列が三角化されるように変換し、変換された行列 $M[2]$ とベクトル $v[2]$ を出力する方程式変換装置である。

【0 0 5 9】

第 2 方程式変換部102は、第 1 初期値設定部1021と、探索部1022と、第 2 初期値設定部1023と、三角化部1024と、第 1 終了判定部1025と、第 2 終了判定部1026を備える。

【0 0 6 0】

第 1 初期値設定部1021は、カウンタ j を1に設定する。

【0 0 6 1】

探索部1022は、第 j 列の成分の中で $GF(p)$ 上で0でない成分を第 j 行から第 n 行まで探索し、はじめに発見した成分の行数を k とする。さらに $k \neq j$ の場合に、行列 $M[2]$ 、 $v[2]$ のそれぞれの第 k 行と第 j 行を入れ換え、行列 $M(j, i, 2)$ 、 $v(j, i, 2)$ とし、出力する。

【0 0 6 2】

第 2 初期値設定部1023は、カウンタ i を $j+1$ に設定する。

【 0 0 6 3 】

三角化部1024は、 $M \downarrow (jj)(M \downarrow (ij))$ は行列 $M(j, i, 2)$ の i 行 j 列成分)と $M \downarrow (ij)$ を用いて、 $j+1 \leq k \leq n$ に対して、

$$M \downarrow (ij) \leftarrow 0$$

$$M \downarrow (ik) \leftarrow M \downarrow (jj) \times M \downarrow (ik) - M \downarrow (ij) \times M \downarrow (jk)$$

$$b \downarrow i \leftarrow M \downarrow (jj) \times b \downarrow i - M \downarrow (ij) \times b \downarrow j$$

のように設定し、設定後の行列を $M(j, i, 3)$ 、ベクトルを $v(j, i, 3)$ とし、出力する。

【 0 0 6 4 】

第1終了判定部1025は、 $i=n$ であるか判定する。

【 0 0 6 5 】

第2終了判定部1026は、 $j=n$ であるか判定する。

【 0 0 6 6 】

以下に、第2方程式変換部102の動作を示す。

【 0 0 6 7 】

第1初期値設定部1021は、カウンタ j を1に設定し、探索部1022に j 、第1方程式変換部101で出力された行列 $M[1]$ 、ベクトル $v[1]$ を入力する。探索部1022は、第 j 列の成分の中で $GF(p)$ 上で0でない成分を j 行、 $j+1$ 行、...、 n 行まで探索し、はじめて発見した成分の行数を k とする。さらに $k \neq j$ の場合に、行列 $M[1]$ 、ベクトル $v[1]$ のそれぞれの第 k 行と第 j 行を入れ換え、入れ換えた後の行列、ベクトルをそれぞれ、 $M(j, i, 2)$ 、 $v(j, i, 2)$ とし、第2初期値設定部1023に j を入力する。第2初期値設定部1023は、 i を $j+1$ に設定し、三角化部1024に $M(j, i, 2)$ 、 $v(j, i, 2)$ を入力する。三角化部1024は、 $M(j, i, 2)$ 、 $v(j, i, 2)$ を変換し、変換後の行列、ベクトルをそれぞれ、 $M(j, i, 3)$ 、 $v(j, i, 3)$ とし、第1終了判定部1025に i を入力する。第1終了判定部1025は、 $i=n$ であるか判定し、 $i=n$ であるとき、第2終了判定部1026に j を入力する。それ以外は、 i を $i+1$ に設定し、三角化部1024に $M(j, i-1, 3)$ 、 $v(j, i-1, 3)$ を入力する。第2終了判定部1026は、 $j=n$ であるか判定し、 $j=n$ であるとき、 $M(j, i-1, 3)$ 、 $v(j, i-1, 3)$ を $M[2]$ 、 $v[2]$ として出力し、終了。それ以外は、 j を $j+1$ に設定し、探索部1022に j 、 $M(j-1, i-1$

、3)、 $v(j-1, i-1, 3)$ を入力する。

【0068】

(第2方程式変換部102の検証)

第2方程式変換部102は、行列を上三角行列になるように変換している。方程式の解を変化させないようにするため、ベクトルも変化させている。従来法と異なる点は、対角成分を1にしないことである。

【0069】

三角化部1024の入力を行列 $M \downarrow (in)$ 、ベクトル $v \downarrow (in)$ とし、出力を行列 $M \downarrow (out)$ 、ベクトル $v \downarrow (out)$ とする。三角化部1024は、行列 $M \downarrow (in)$ の第 i 、 j 行の行ベクトルをそれぞれ、 $l \downarrow i$ 、 $l \downarrow j$ とすると、

$$M \downarrow (jj) \times l \downarrow i - M \downarrow (ij) \times l \downarrow j$$

の計算を行い、この結果の行ベクトルを $M \downarrow (out)$ の第 i 行とし、

$$M \downarrow (jj) \times b \downarrow i - M \downarrow (ij) \times b \downarrow j$$

の計算を行い、 $v \downarrow (out)$ の第 i 行としている。他の $M \downarrow (out)$ 、 $v \downarrow (out)$ の成分は $M \downarrow (in)$ 、 $v \downarrow (in)$ と同じである。このとき、方程式

$$M \downarrow (in) \cdot x[1] = v \downarrow (in)$$

と方程式

$$M \downarrow (out) \cdot x[1] = v \downarrow (out)$$

が同じ解をもつことは、以下の文献から明らかである。

【0070】

水上孝一編著、「コンピュータによる数値計算」、プログラミング入門シリーズ、朝倉書店、1985、76～82ページ

以上より、第2方程式変換部102の方程式変換によって、解は変化しない。

【0071】

また、三角化部1024にあるようにカウンタ j に対して、 $j+1 \leq i \leq n$ を満たす i に対して、 $M \downarrow (ij)$ が0になる。この操作を j が1から n まで繰り返すので、行列の下三角部分が0になる。したがって、第2方程式変換部102は方程式の解を変化させずに、行列の三角化変換が行える。

【0072】

(逆元演算部103の構成)

図 3 は、逆元演算部103の構成を示すブロック図である。

【 0 0 7 3 】

逆元演算部103は、第 2 方程式変換部102から出力された行列の対角成分 $m \downarrow k$ ($1 \leq k \leq n$)のGF(p)上の逆元を計算し、出力する逆元演算装置である。

【 0 0 7 4 】

逆元演算部103は、乗算部1031と、第 1 逆元演算部1032と、第 2 逆元演算部1033を備える。

【 0 0 7 5 】

乗算部1031は、

$$t \downarrow i = \Pi \downarrow (k \neq i) \ m \downarrow k \ \text{mod } p \quad (i=1, 2, \dots, n)$$

を

$$s \downarrow 1 = m \downarrow 1 \times m \downarrow 2 \ \text{mod } p$$

$$s \downarrow 2 = s \downarrow 1 \times m \downarrow 3 \ \text{mod } p$$

...

$$s \downarrow (n-3) = s \downarrow (n-4) \times m \downarrow (n-2) \ \text{mod } p$$

$$t \downarrow n = s \downarrow (n-3) \times m \downarrow (n-1) \ \text{mod } p$$

$$t \downarrow (n-1) = s \downarrow (n-3) \times m \downarrow n \ \text{mod } p$$

$$s \downarrow n = m \downarrow (n-1) \times m \downarrow n \ \text{mod } p, \ t \downarrow (n-2) = s \downarrow (n-4) \times s \downarrow n \ \text{mod } p$$

$$s \downarrow (n-1) = m \downarrow (n-2) \times s \downarrow n \ \text{mod } p, \ t \downarrow (n-3) = s \downarrow (n-5) \times s \downarrow (n-1) \ \text{mod } p$$

$$s \downarrow (n-2) = m \downarrow (n-3) \times s \downarrow (n-1) \ \text{mod } p, \ t \downarrow (n-4) = s \downarrow (n-6) \times s \downarrow (n-2) \ \text{mod } p$$

...

$$s \downarrow 5 = m \downarrow 4 \times s \downarrow 6 \ \text{mod } p, \ t \downarrow 3 = s \downarrow 1 \times s \downarrow 5 \ \text{mod } p$$

$$s \downarrow 4 = m \downarrow 3 \times s \downarrow 5 \ \text{mod } p, \ t \downarrow 2 = m \downarrow 1 \times s \downarrow 4 \ \text{mod } p$$

$$t \downarrow 1 = m \downarrow 2 \times s \downarrow 4 \ \text{mod } p$$

のように求め、

$$t = \Pi \downarrow k \ m \downarrow k \ \text{mod } p$$

を予め与えられたkを用いて、

$$t = t \downarrow k \times m \downarrow k \ \text{mod } p$$

のように求める。

【0076】

第1逆元演算部1032は、

$$u = 1/t \bmod p$$

を計算する。

【0077】

第2逆元演算部1033は、

$$I \downarrow i = u \times t \downarrow i \bmod p \quad (i=1, 2, \dots, n)$$

を計算する。

【0078】

以下に逆元演算部103の動作を示す。

【0079】

乗算部1031は、 $t \downarrow i = \prod \downarrow (k \neq i) \ m \downarrow k \bmod p \ (1 \leq i \leq n)$ と、 $t = \prod \downarrow k \ m \downarrow k \bmod p$ を計算し、第1逆元演算部1032に t を入力する。第1逆元演算部1032は、 t のGF(p)上の逆元を計算し、それを u とし、 u 、 $t \downarrow i \ (1 \leq i \leq n)$ を第2逆元演算部1033に入力する。第2逆元演算部1033は、 $m \downarrow i \ (1 \leq i \leq n)$ のGF(p)上の逆元 $I \downarrow i$ を計算し、出力する。

【0080】

(逆元演算部103の動作の検証)

乗算部1031では、

$$s \downarrow 1 = m \downarrow 1 \times m \downarrow 2 \bmod p$$

$$s \downarrow 2 = s \downarrow 1 \times m \downarrow 3 = m \downarrow 1 \times m \downarrow 2 \times m \downarrow 3 \bmod p$$

$$s \downarrow 3 = s \downarrow 2 \times m \downarrow 4 = m \downarrow 1 \times m \downarrow 2 \times m \downarrow 3 \times m \downarrow 4 \bmod p$$

...

$$s \downarrow (n-3) = m \downarrow 1 \times m \downarrow 2 \times m \downarrow 3 \times \dots \times m \downarrow (n-2) \bmod p$$

$$t \downarrow n = s \downarrow (n-3) \times m \downarrow (n-1) = m \downarrow 1 \times m \downarrow 2 \times m \downarrow 3 \times \dots \times m \downarrow (n-1) = \prod \downarrow (k \neq n) \ m \downarrow k \bmod p$$

で、 $t \downarrow n$ を求める。

【0081】

$t \downarrow (n-1) = s \downarrow (n-3) \times m \downarrow n = m \downarrow 1 \times m \downarrow 2 \times m \downarrow 3 \times \dots \times m \downarrow (n-2) \times m \downarrow n = \Pi \downarrow (k \neq n-1) \ m \downarrow k \bmod p$

で、 $t \downarrow (n-1)$ を計算し、

$$s \downarrow n = m \downarrow (n-1) \times m \downarrow n = \bmod p$$

$t \downarrow (n-2) = s \downarrow (n-4) \times s \downarrow n = m \downarrow 1 \times m \downarrow 2 \times m \downarrow 3 \times \dots \times m \downarrow (n-3) \times m \downarrow (n-1) \times m \downarrow n = \Pi \downarrow (k \neq n-2) \ m \downarrow k \bmod p$

で、 $t \downarrow (n-2)$ を計算する。

【0 0 8 2】

以下、同様にして、

$t \downarrow (n-3)$ から $t \downarrow 2$ まで計算する。

【0 0 8 3】

さらに、

$$t \downarrow 1 = m \downarrow 2 \times s \downarrow 4 = m \downarrow 2 \times m \downarrow 3 \times \dots \times m \downarrow n = \Pi \downarrow (k \neq 1) \ m \downarrow k \bmod p$$

で、 $t \downarrow 1$ を求め、これまでに求めた $t \downarrow k (1 \leq k \leq n)$ のいずれかを用いて、

$$t = t \downarrow k \times m \downarrow k \bmod p$$

を計算する。

【0 0 8 4】

第1逆元演算部1032で、 t の逆元 u を求める。

【0 0 8 5】

第2逆元演算部1033では、

$$u = 1 / (m \downarrow 1 \times m \downarrow 2 \times m \downarrow 3 \times \dots \times m \downarrow n) \bmod p$$

であり、 $t \downarrow i = \Pi \downarrow (k \neq i) \ m \downarrow k \bmod p (1 \leq i \leq n)$ であるので、

$$1 / m \downarrow i = u \times t \downarrow i \bmod p$$

が成り立つことを利用して、 $m \downarrow i$ の逆元 $1 \downarrow i$ を求める。以上より、すべての $m \downarrow i (1 \leq i \leq n)$ の逆元 $1 \downarrow i$ が得られる。

【0 0 8 6】

(方程式求解部104の構成)

図4は、方程式求解部104の構成を示すブロック図である。

【0 0 8 7】

方程式求解部104は、第2方程式変換部102から出力された行列 $M[2]$ とベクトル $v[2]$ と逆元演算部103から出力された逆元 $I \downarrow i (1 \leq i \leq n)$ を用いて、方程式の解を求め出力する。以下では、解を $y \downarrow i$ とする。

【0088】

方程式求解部104は、初期値設定部1041と、求解部1042と、終了判定部1043を備える。

【0089】

初期値設定部1041は、カウンタ c を n に設定する。

【0090】

求解部1042は、 $y \downarrow c$ を次のように計算する。

【0091】

$$y \downarrow c = I \downarrow c \times b \downarrow c - \sum_{i=c+1}^n (M \downarrow (ci) \times y \downarrow i)$$

ここで、 $M \downarrow (ij)$ は、行列 $M[2]$ の第 i 行第 j 列成分であり、 $b \downarrow i$ はベクトル $v[2]$ の第 i 行成分である。

【0092】

終了判定部1043は、 $c=0$ であるか判定する。

【0093】

以下に方程式求解部104の動作を示す。

【0094】

初期値設定部1041は、 c を n に設定し、求解部1042に c と第2方程式変換部102から出力された $M[2]$ 、 $v[2]$ と逆元演算部103から出力された $I \downarrow c$ を入力する。求解部1042は、 $y \downarrow c$ を求め、終了判定部1043に c を入力する。終了判定部1043は、 $c=0$ であるか判定し、 $c=0$ であるとき、解 $y \downarrow k (1 \leq k \leq n)$ を出力する。それ以外は、 c を $c+1$ に設定し、求解部1042に $M[2]$ 、 $v[2]$ 、 $I \downarrow c$ を入力する。

【0095】

(方程式求解部104の検証)

第2方程式変換102から出力された行列 $M[2]$ は上三角化行列であるので、方程式

$$M[2] \cdot x[1] = v[2]$$

は、

$$M \downarrow (11) \times x \downarrow 1 + M \downarrow (12) \times x \downarrow 2 + M \downarrow (13) \times x \downarrow 3 + \dots + M \downarrow (1n) \times x \downarrow n = b \downarrow 1$$

$$M \downarrow (22) \times x \downarrow 2 + M \downarrow (23) \times x \downarrow 3 + \dots + M \downarrow (2n) \times x \downarrow n = b \downarrow 2$$

...

$$M \downarrow (nn) \times x \downarrow n = b \downarrow n$$

の形をしている。また、行列の対角成分の逆元を求めているので、 $x \downarrow n$ の解 $y \downarrow n$

は、

$$y \downarrow n = I \downarrow n \times b \downarrow n \bmod p$$

であり、 $x \downarrow (n-1)$ の解 $y \downarrow (n-1)$ は、

$$y \downarrow (n-1) = I \downarrow (n-1) \times b \downarrow (n-1) - M \downarrow (n-1, n) \times y \downarrow n$$

である。同様にして、 $x \downarrow c$ の解 $y \downarrow c$ は、

$$y \downarrow c = I \downarrow c \times b \downarrow c - \sum \downarrow (c+1 \leq i \leq n) (M \downarrow (ci) \times y \downarrow i)$$

である。

【0096】

以上の各部の検証より、本実施形態1の有限体上の演算装置は、有限体上の連立方程式の解を求めることができる。

【0097】

(実施形態1の効果)

この例の計算量について説明する。以下で、従来の方法との比較を行う。

【0098】

基礎体GF(p)の乗算、逆元演算の計算量をそれぞれ、Mul、Invとする。従来の方法では、従来例3に示すような方法を用いて連立方程式の解を求めている。この場合、計算量は $1/3 \times n \times (n \uparrow 2 + 3 \times n - 1) \times \text{Mul} + n \times \text{Inv}$ である。本実施形態1では、三角化部102の計算量が、 $2/3 \times n \times (n-1) \times (n+1) \times \text{Mul}$ であり、逆元演算部の計算量が $(4 \times n - 5) \times \text{Mul} + \text{Inv}$ 、方程式求解部104の計算量が $1/2 \times n \times (n+1) \times \text{Mul}$ であるので、逆元演算装置10全体の計算量は、 $(2/3 \times n \uparrow 3 + 1/2 \times n \uparrow 2 + 23/6 \times n - 5) \times \text{Mul} + \text{Inv}$ である。 $n=5$ 、 $|q|=160$ ($|q|$ は q のビットサイズ)の場合、一般的な計算機では、 $\text{Inv}=40\text{Mul}$ であることが知られているので、従来法の計算量が、 $265 \times \text{Mul}$ であり、本実施形態1では、 $150 \times \text{Mul}$ である。したがって、連立方程式求解が

高速な有限体上の演算装置を提供することができ、この実用的価値は非常に大きい。なお、本実施形態1を用いた暗号システム並びに、誤り訂正システムが実現可能となる。

【0099】

(実施形態2)

図5は、実施形態2における逆元演算装置の構成を示すブロック図である。

【0100】

この逆元演算装置は、予め与えられた有限体GF(p)の拡大体GF(q) ($q=p \uparrow n$)において、GF(q)の元xを入力とし、xのGF(q)上の逆元Iを出力する。以下では、拡大体GF(q)の生成多項式を $g \uparrow n-\beta$ とし、その根を α 、 $x=x \downarrow 0+x \downarrow 1 \times \alpha + \dots + x \downarrow (n-1) \times \alpha \uparrow (n-1)$ とする。

【0101】

逆元演算装置20は、方程式生成部201と、方程式計算部202と、逆元変換部203を備える。

【0102】

方程式生成部201は、xから以下の $y \downarrow i$ ($0 \leq i \leq n-1$)に関する連立方程式を生成する。

【0103】

$$x \downarrow 0 \times y \downarrow 0 + \beta \times x \downarrow (n-1) \times y \downarrow 1 + \beta \times x \downarrow (n-2) \times y \downarrow 2 + \dots + \beta \times x \downarrow 1 \times y \downarrow (n-1) = 1$$

$$x \downarrow 1 \times y \downarrow 0 + x \downarrow 0 \times y \downarrow 1 + \beta \times x \downarrow (n-1) \times y \downarrow 2 + \dots + \beta \times x \downarrow 2 \times y \downarrow (n-1) = 0$$

$$x \downarrow 2 \times y \downarrow 0 + x \downarrow 1 \times y \downarrow 1 + x \downarrow 0 \times y \downarrow 2 + \dots + \beta \times x \downarrow 3 \times y \downarrow (n-1) = 0$$

...

$$x \downarrow (n-1) \times y \downarrow 0 + x \downarrow (n-2) \times y \downarrow 1 + x \downarrow (n-3) \times y \downarrow 2 + \dots + x \downarrow 0 \times y \downarrow (n-1) = 0$$

方程式計算部202は、実施形態1の有限体の演算装置と同一である。

【0104】

逆元変換部203は、方程式計算部202から出力された解 $y \downarrow k$ ($1 \leq k \leq n$)を逆元Iに以下のように変換する。

【0105】

$$I = y \downarrow 0 + y \downarrow 1 \times \alpha + \dots + y \downarrow (n-1) \times \alpha \uparrow (n-1)$$

以下に逆元演算装置20の動作を示す。

【0106】

方程式生成部201は、 x と $GF(q)$ の生成多項式から連立方程式を生成し、その方程式のパラメータを方程式計算部202に入力する。方程式計算部202は、方程式の解を求め、その解を逆元変換部203に入力する。逆元変換部203は、方程式の解を逆元に変換し、出力する。

【0107】

(実施形態2の検証)

本実施形態2の I と x について、

$$x \times I = 1 \bmod f(g)$$

という関係式であるとき、

$$\begin{aligned} x \times I &= x \downarrow 0 \times (y \downarrow 0 + y \downarrow 1 \times \alpha + \dots + y \downarrow (n-1) \times \alpha \uparrow (n-1)) \\ &\quad + x \downarrow 1 \times \alpha \times (y \downarrow 0 + y \downarrow 1 \times \alpha + \dots + y \downarrow (n-1) \times \alpha \uparrow (n-1)) \\ &\quad + x \downarrow 2 \times \alpha \uparrow 2 \times (y \downarrow 0 + y \downarrow 1 \times \alpha + \dots + y \downarrow (n-1) \times \alpha \uparrow (n-1)) \\ &\quad \dots \\ &\quad + x \downarrow (n-1) \times \alpha \uparrow (n-1) \times (y \downarrow 0 + y \downarrow 1 \times \alpha + \dots + y \downarrow (n-1) \times \alpha \uparrow (n-1)) \end{aligned}$$

であり、

$$\alpha \uparrow n = \beta \bmod f(g)$$

であるので、

$$\begin{aligned} x \times I &= x \downarrow 0 \times (y \downarrow 0 + y \downarrow 1 \times \alpha + \dots + y \downarrow (n-1) \times \alpha \uparrow (n-1)) \\ &\quad + x \downarrow 1 \times (y \downarrow 0 \times \alpha + y \downarrow 1 \times \alpha \uparrow 2 + \dots + y \downarrow (n-1) \times \beta) \\ &\quad + x \downarrow 2 \times (y \downarrow 0 \times \alpha \uparrow 2 + y \downarrow 1 \times \alpha \uparrow 3 + \dots + y \downarrow (n-1) \times \alpha \times \beta) \\ &\quad \dots \\ &\quad + x \downarrow (n-1) \times (y \downarrow 0 \times \alpha \uparrow (n-1) + y \downarrow 1 \times \beta + \dots + y \downarrow (n-1) \times \alpha \uparrow (n-2) \beta) \end{aligned}$$

であり、 α の降幂の順に整理すると

$$\begin{aligned} x \times I &= x \downarrow 0 \times y \downarrow 0 + \beta \times x \downarrow (n-1) \times y \downarrow 1 + \dots + \beta \times x \downarrow 1 \times y \downarrow (n-1) \\ &\quad + \alpha \times (x \downarrow 1 \times y \downarrow 0 + x \downarrow 0 \times y \downarrow 1 + \dots + \beta \times x \downarrow 2 \times y \downarrow (n-1)) \\ &\quad + \alpha \uparrow 2 \times (x \downarrow 2 \times y \downarrow 0 + x \downarrow 1 \times y \downarrow 1 + \dots + \beta \times x \downarrow 3 \times y \downarrow (n-1)) \end{aligned}$$

...

$$+ \alpha \uparrow (n-1) \times (x \downarrow (n-1) \times y \downarrow 0 + x \downarrow (n-2) \times y \downarrow 1 + \dots + x \downarrow 0 \times y \downarrow (n-1))$$

である。これが1に等しいので、方程式生成部201によって生成された方程式が導くことができる。したがって、拡大体GF(q)の逆元を求めることは、基礎体GF(p)上の連立方程式を解くことと等しい。

【0108】

また、上記例では、 $g \uparrow n - \beta$ の形の生成多項式を扱ったが、一般の生成多項式に対しても同様の操作により、方程式を生成できる。

【0109】

(実施形態2の効果)

この例の計算量については、実施形態1で述べたとおりである。本実施形態2によって、高速な逆元演算装置を実現可能となり、実用的価値は非常に大きい。なお、本実施形態2を用いた暗号システム並びに、誤り訂正システムが実現可能となる。

【0110】

【発明の効果】

以上に説明したように本発明は、従来例における問題点を鑑みて行われたもので、有限体上の連立方程式求解及び、拡大体上の逆元演算の計算時間を短縮できた。

【0111】

以上により、高速な暗号方式や署名方式を可能にする有限体上の演算装置及び、逆元演算装置を提供することができ、その実用的価値は大きい。

【図面の簡単な説明】

【図1】

本発明の実施形態1の有限体上の演算装置のブロック図

【図2】

本発明の実施形態1の第2方程式変換部のブロック図

【図3】

本発明の実施形態1の逆元演算部のブロック図

【図 4】

本発明の実施形態 1 の方程式求解部のブロック図

【図 5】

本発明の実施形態 2 の逆元演算装置のブロック図

【図 6】

従来例 1 のエルガマル署名によるデジタル署名方式の手順を示すシーケンス図

【図 7】

従来例 2 の逆元演算装置のブロック図

【図 8】

従来例 3 の連立方程式の求解装置のブロック図

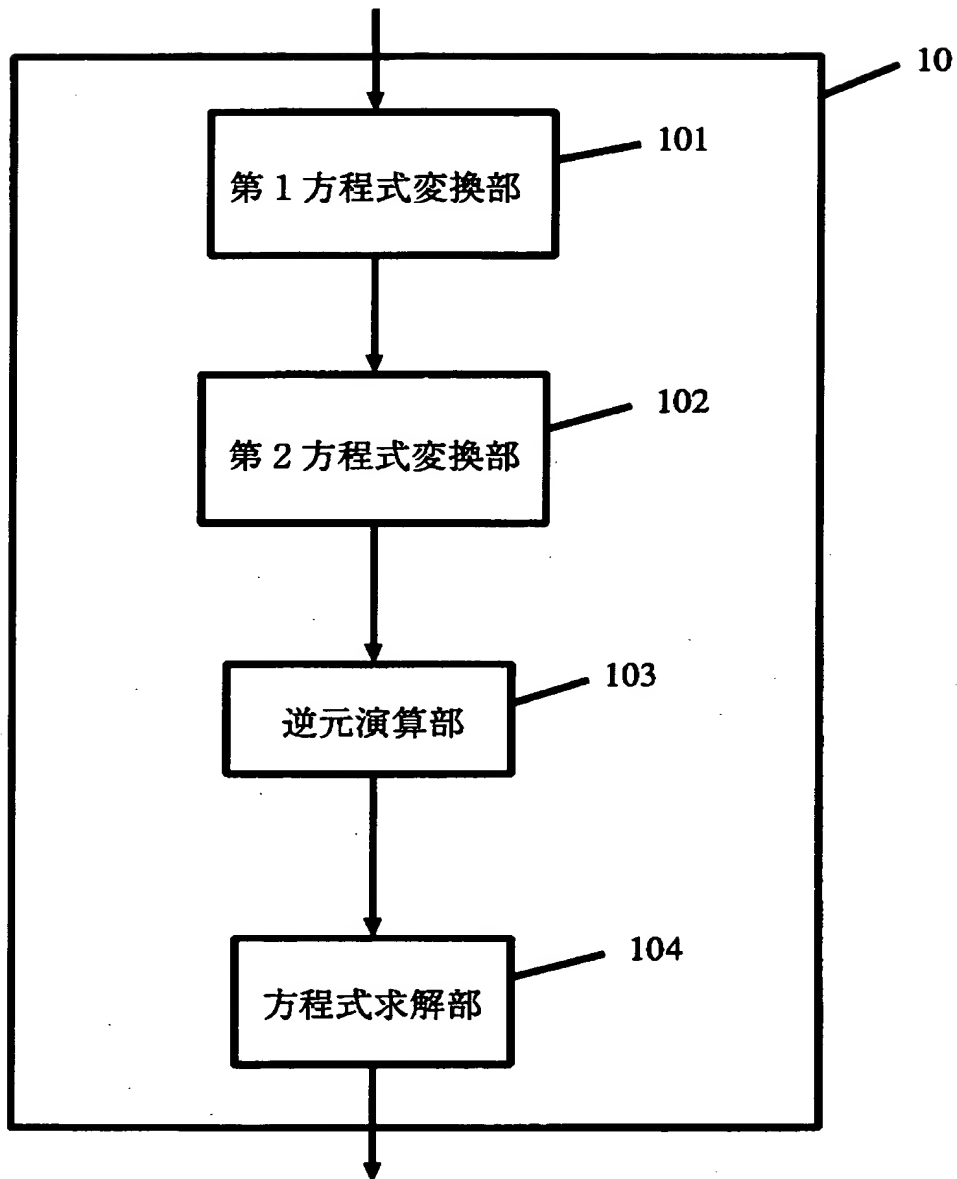
【符号の説明】

- 1 0 本発明の実施形態 1 の有限体上の演算装置
- 1 0 1 第 1 方程式変換部
- 1 0 2 第 2 方程式変換部
- 1 0 2 1 第 1 初期値設定部
- 1 0 2 2 探索部
- 1 0 2 3 第 2 初期値設定部
- 1 0 2 4 三角化部
- 1 0 2 5 第 1 終了判定部
- 1 0 2 6 第 2 終了判定部
- 1 0 3 逆元演算部
- 1 0 3 1 乗算部
- 1 0 3 2 第 1 逆元演算部
- 1 0 3 3 第 2 逆元演算部
- 1 0 4 方程式求解部
- 1 0 4 1 初期値設定部
- 1 0 4 2 求解部
- 1 0 4 3 終了判定部

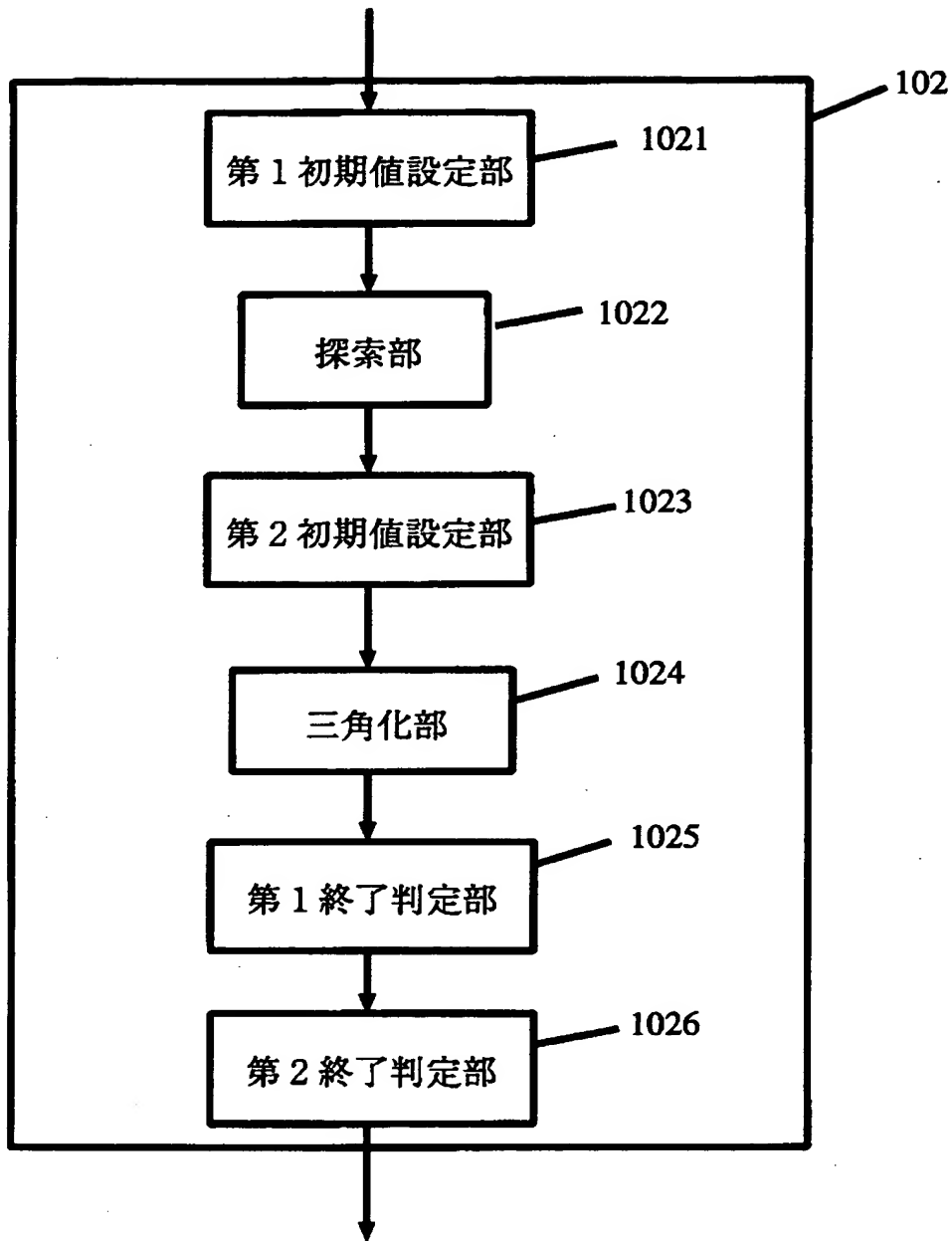
【書類名】

図面

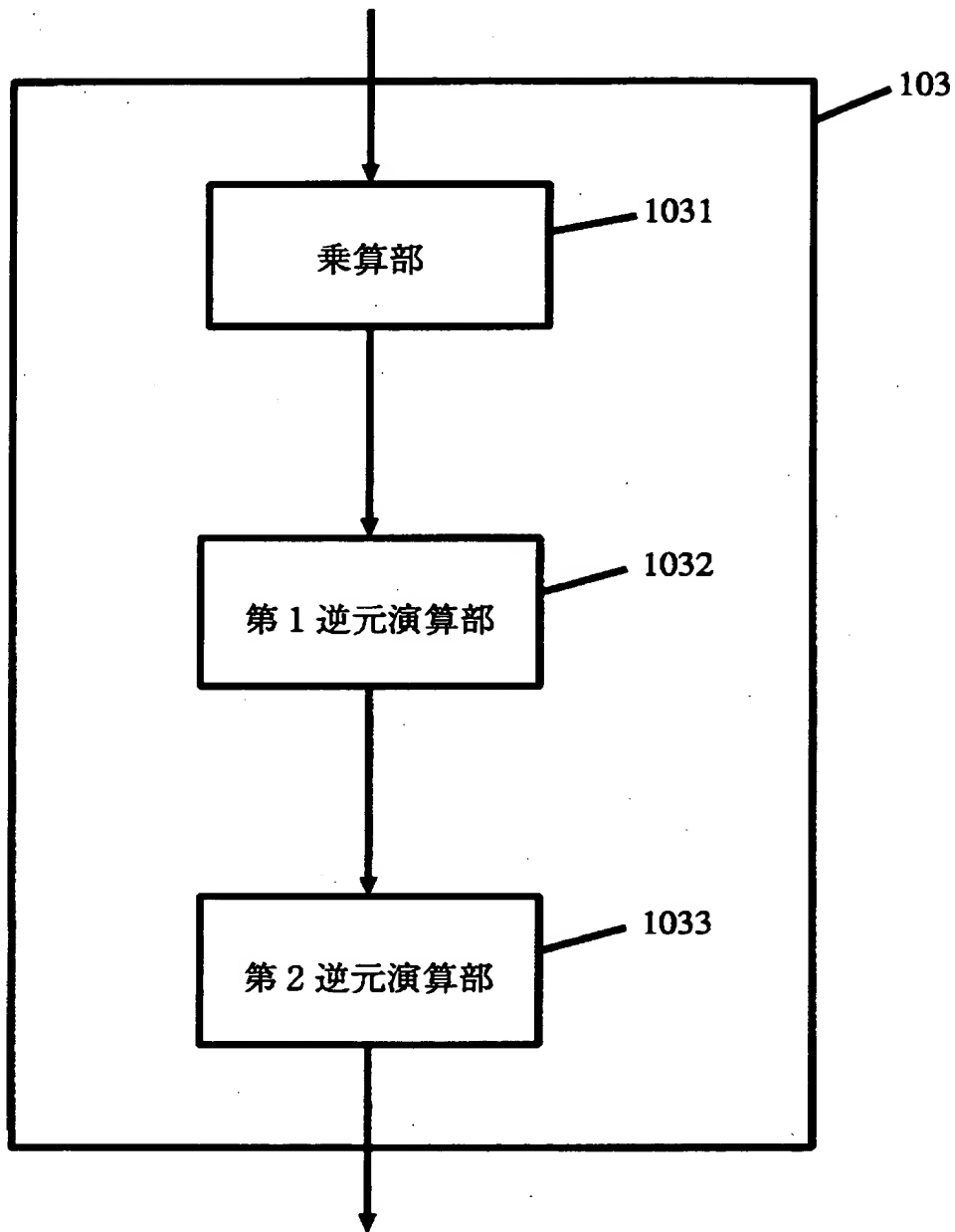
【図 1】



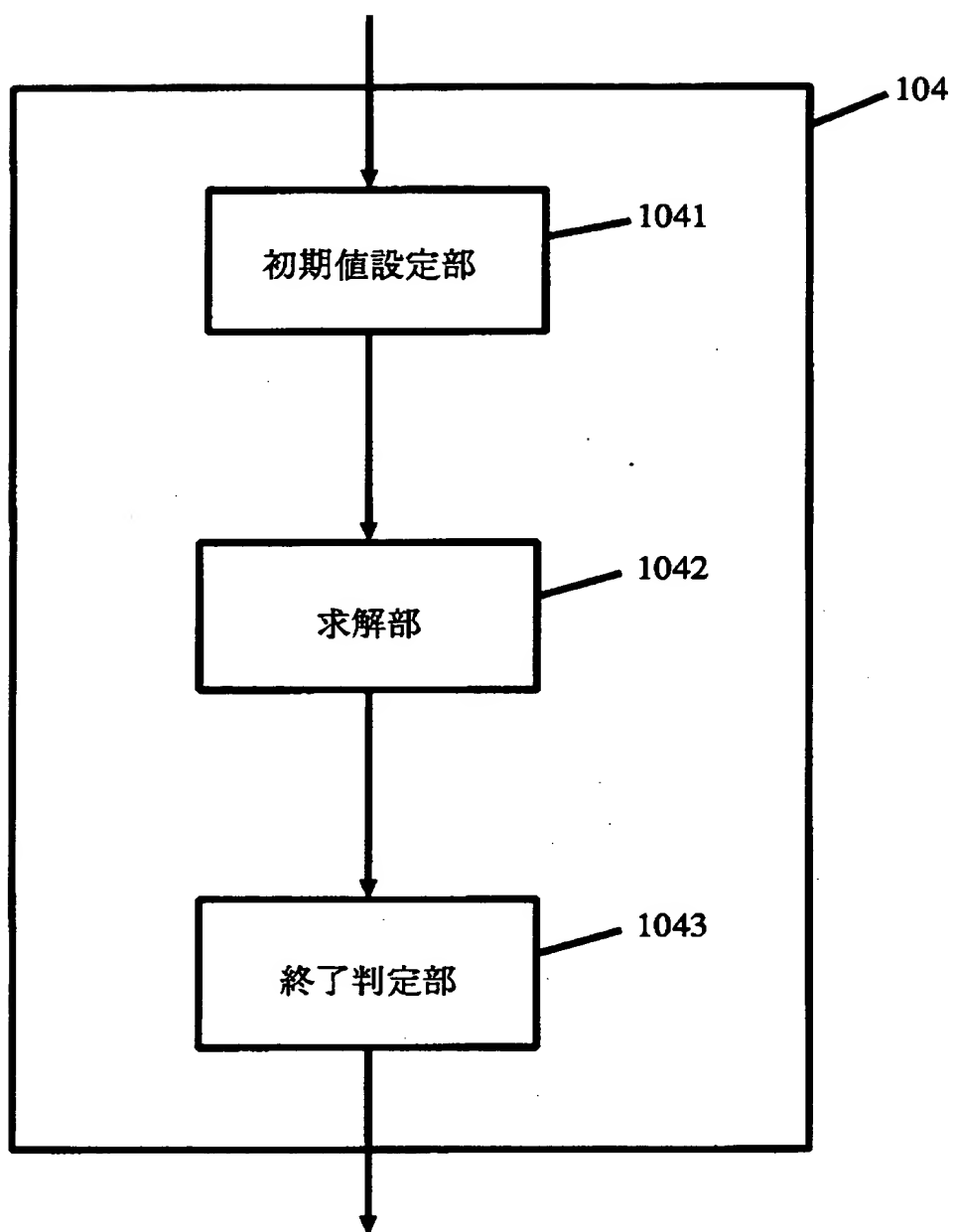
【図 2】



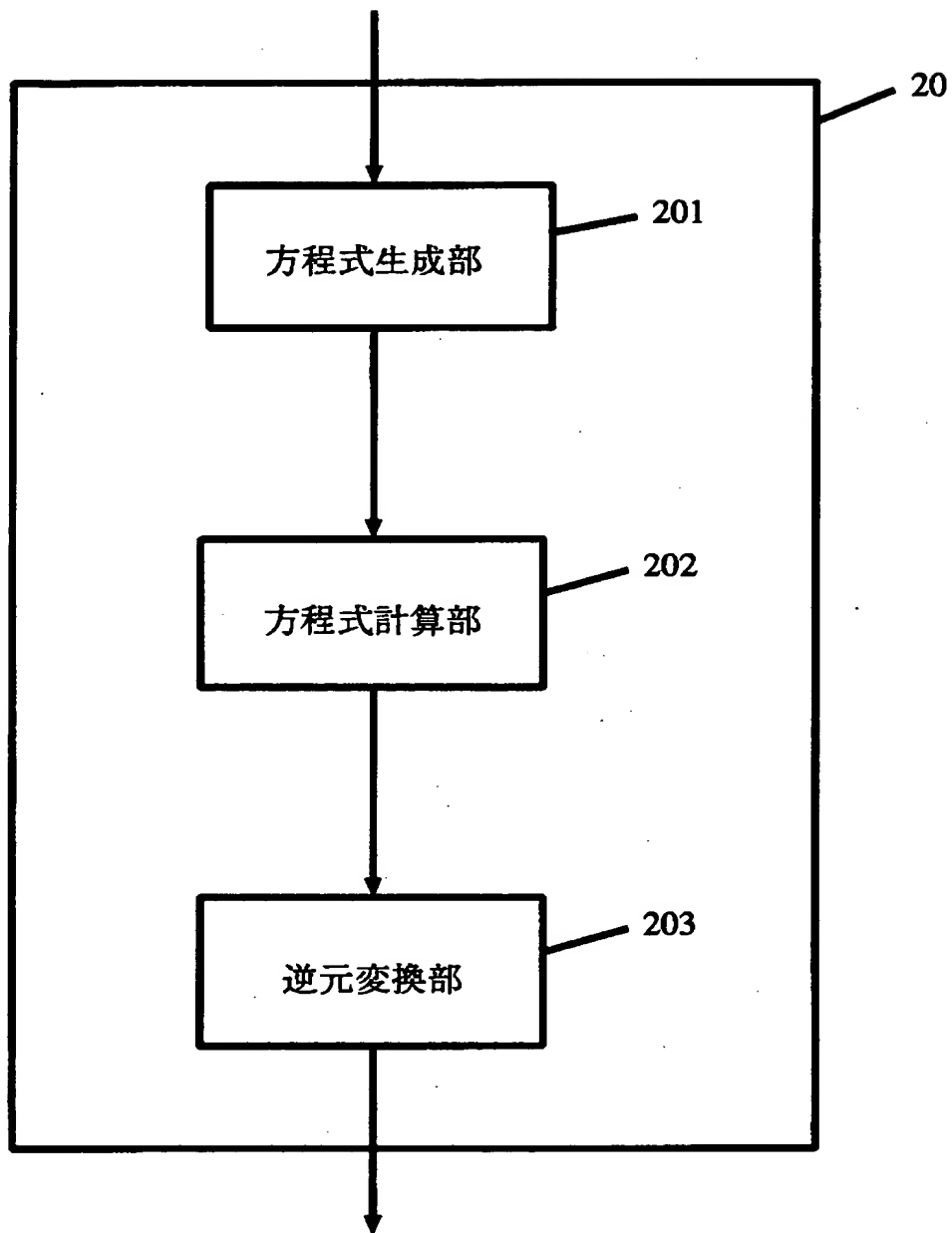
【図 3】



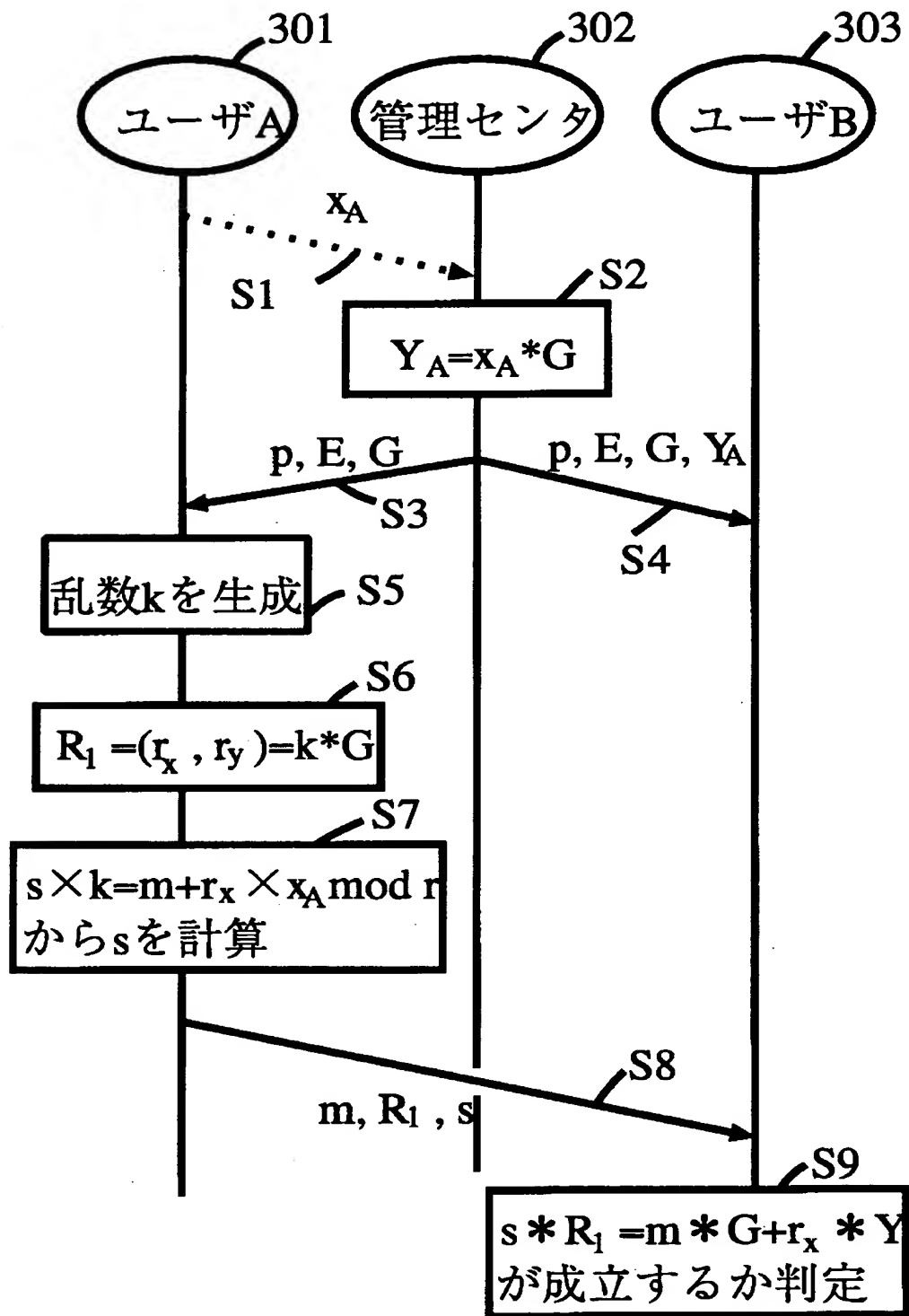
【図 4】



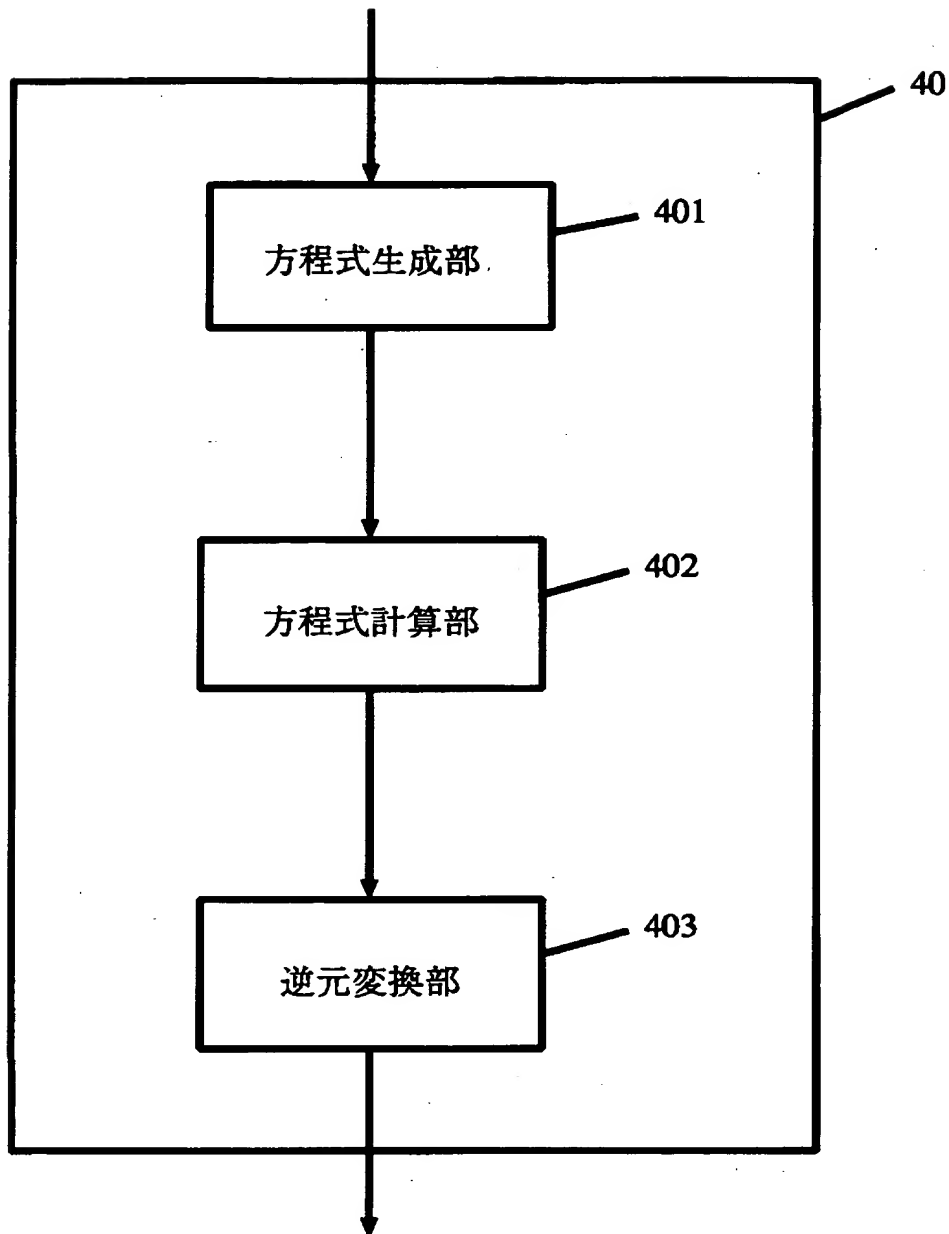
【図 5】



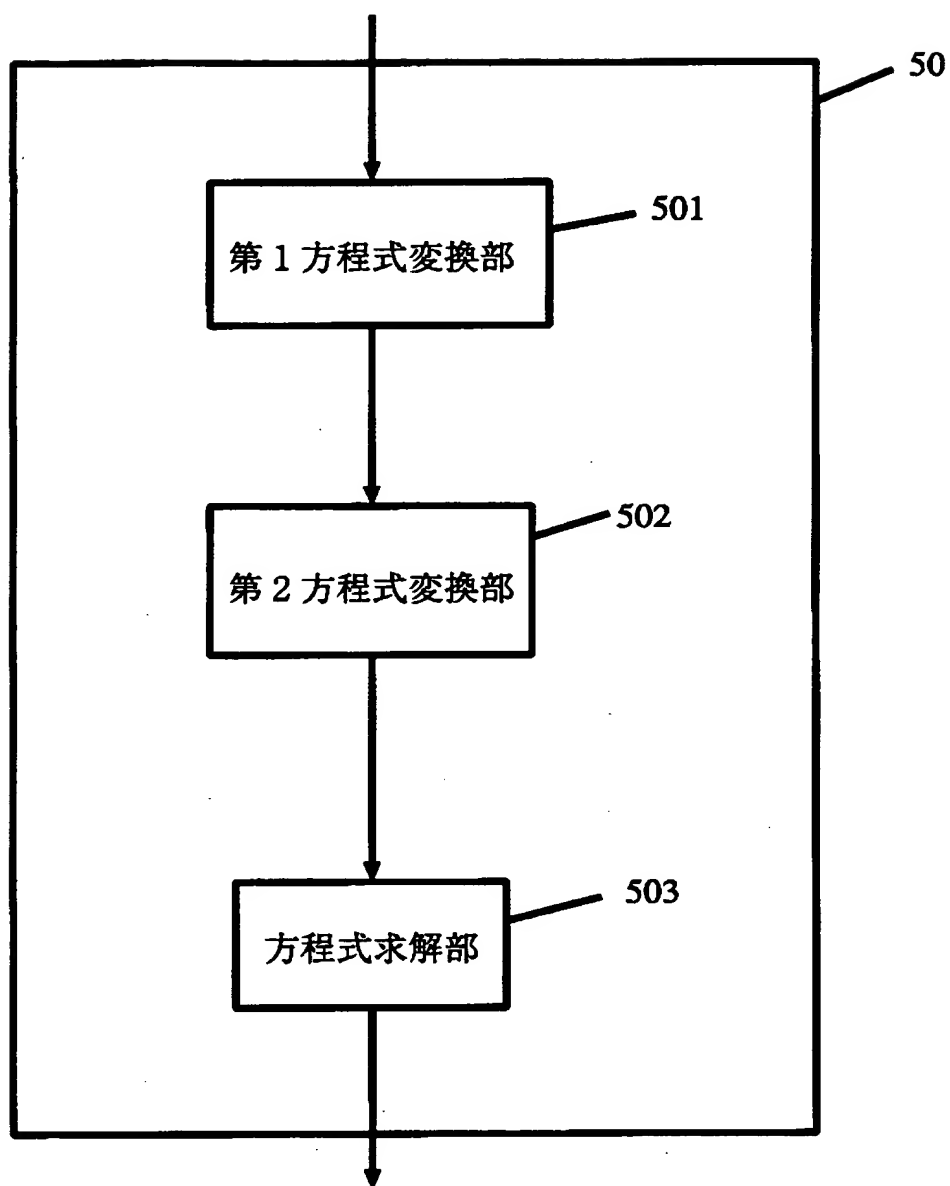
【図6】



【図 7】



【図 8】



【書類名】 要約書

【要約】

【課題】 高速に有限体上の連立方程式の解を求める有限体上の演算装置を提供することにより、拡大体の逆元演算の計算時間を短縮し、高速な暗号システムを構築することを目的とする。

【解決手段】 本発明は、有限体 $GF(p)$ (p :素数)の連立方程式の解を求める有限体上の演算装置であって、連立方程式を行列とベクトルで表現する第1方程式変換部と、前記行列を三角化変換する第2方程式変換部と、三角行列の対角成分の $GF(p)$ 上の逆元を求める逆元演算部と、三角行列及びベクトルと、前記逆元を用いて前記連立方程式の解を求める方程式求解部を備え、前記第2方程式変換部では、前記有限体の逆元演算を行わないことを特徴とする。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日
[変更理由] 新規登録
住 所 大阪府門真市大字門真1006番地
氏 名 松下電器産業株式会社